IN THE CLAIMS

1. [currently amended, previously amended] A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said intermediate computer devices may perform ~~performs~~ a network address translation or ~~and/or~~ a protocol conversion resulting in alteration of a packet propagating therethrough, the method comprising the steps of

- determining what network address translations or ~~and/or~~ protocol conversions, if any, occur on packets transmitted in a data path between said ~~the~~ first computer device and ~~the~~ said second computer device on packets transmitted between said first computer device and said second computer device,
- if it is found that network address translations or ~~and/or~~ protocol conversions occur in said ~~a~~ data path between said first computer device and said ~~a~~ second computer device, taking packets conforming to a first protocol and using said first computer device to encapsulate ~~encapsulating~~ them into packets conforming to a second protocol, ~~which~~ said second protocol being ~~is~~ capable of traversing network address translations and ~~and/or~~ protocol conversions,
- transmitting said packets conforming to said second protocol from said first computer device to said second computer device; and
- decapsulating said transmitted packets conforming to said second protocol into packets conforming to said first protocol.

2. [original] A method according to claim 1, wherein the step of taking packets conforming to a first protocol and encapsulating them into packets conforming to a

second protocol comprises the substeps of

- taking packets conforming to the Internet Protocol,
- processing said packets according to the IPSEC protocol suite and
- encapsulating the processed packets into packets conforming to the User Datagram Protocol.

3. [original] A method according to claim 1, wherein the step of taking packets conforming to a first protocol and encapsulating them into packets conforming to a second protocol comprises the substeps of

- taking packets conforming to the Internet Protocol,
- processing said packets according to the IPSEC protocol suite and
- encapsulating the processed packets into packets conforming to the Transmission Control Protocol.

4. [previously amended] A method according to claim 1, further comprising the step of compensating for the network address translations on said second protocol in the packets that are transmitted from said first computer device to said second computer device.

5. [previously amended] A method according to claim 4, wherein said step of compensating for said network address translations comprises a step of performing address translation based on the information obtained in the step of determining what network address translations, if any, occur on packets transmitted between said first computer device and said second computer device.

6. [previously amended] A method according to claim 5, wherein said step of compensating for said network address translations further comprises a step of performing port number translation based on the information obtained in the step of determining what network address translations, if any, occur on packets transmitted between said first computer device and said second computer device.

7. [previously amended] A method according to claim 1, additionally comprising the step of periodically transmitting keepalive packets between said first computer device and said second computer device to ensure that said network address translations, if any, occurring on packets transmitted between said first computer device and said second computer device stay the same.

8. [currently amended, previously amended] A method for conditionally setting up a secure communication connection between a first computer device and a second computer device through a packet-switched data transmission network including intermediate computer devices, where at least one of said computer devices performs a network address translation ~~and/or~~ or a protocol conversion or both a protocol conversion and a network address translation, the method comprising the steps of

- finding out, whether or not said second computer device supports a communication method where:

it is determined what network address translations or ~~and/or~~ protocol conversions or both, if any, occur on packets transmitted between said first computer device and said second computer device;

if it is found that network address translations or protocol conversions occur on packets transmitted between said first computer

device and said second computer device, packets are taken that conform to a first protocol and encapsulated into packets that conform to a second protocol, which second protocol is capable of traversing network address translations and/or protocol conversions;

said packets conforming to said second protocol are transmitted from said first computer device to said second computer device;

and said transmitted packets conforming to said second protocol are decapsulated into packets conforming to said first protocol,

- as a response to a finding indicating that the second computer device supports said communication method, setting up a secure communication connection between said first computer device and said second computer device in which communication connection said communication method is employed and

- as a response to a finding indicating that said second computer device does not support said communication method, disabling use of said communication method between said first and said second computer devices.

9. [previously amended] A method for tunnelling packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion, the method comprising the steps of

- establishing a bidirectional tunnelling mode between said first computer device and said second computer device by exchanging packets conforming to a secure communication protocol,

- determining if one or more network address translations and/or protocol

conversions occur on packets travelling from said first computer to said second computer, and if so, taking packets conforming to a first protocol and encapsulating them at said first computer device into packets conforming to a second protocol, which second protocol is capable of traversing network address translations,

- transmitting said packets conforming to said second protocol from said first computer device to said second computer device,

- decapsulating said transmitted packets conforming to said second protocol into packets conforming to said first protocol at the second computer device,

- obtaining information about the address translations occurred on packets transmitted between said first computer device and said second computer device and

- using said obtained information to modify the established bidirectional tunnelling mode between said first computer device and said second computer device.

10. [previously amended] A method according to claim 9, wherein the step of obtaining information about the address translations occurred on packets transmitted between said first computer device and said second computer device comprises the substeps of

- transmitting a packet between said first computer device and said second computer device, said packet comprising a header part and a payload part, and

- comparing a network address transmitted in said payload part to a network address transmitted in said header part in order to find out what changes have occurred on said network address transmitted in said header part.

11. [previously amended] A method according to claim 9, additionally comprising the step of periodically transmitting keepalive packets between said first computer device and said second computer device to ensure that network address translations, if any, occurring on packets transmitted between said first computer device and said second computer device stay the same.

12. [previously amended] A method according to claim 9, wherein the step of using said obtained information to modify the operation of the tunnelling of packets comprises the substep of introducing an address translation before the encapsulation of packets in order to compensate for the network address translations that occur on packets transmitted between said first computer device and said second computer device.

13. [previously amended] A method according to claim 9, wherein the step of using said obtained information to modify the operation of the tunnelling of packets comprises the substep of introducing an address translation after the decapsulation of packets in order to compensate for the network address translations that occur on packets transmitted between said first computer device and said second computer device.

14. [previously amended] A method for tunnelling packets between a first computer device and a second computer device through a packet-switched data transmission network including intermediate computer devices, in which data transmission network there exists a security protocol comprising a key management connection that employs a specific packet format for key management packets, the

method comprising the steps of

- encapsulating data packets that are not key management packets into said specific packet format for key management packets,
- transmitting said data packets encapsulated into the specific packet format from said first computer device to said second computer device,
- discriminating at said second computer device the data packets encapsulated into the specific packet format from actual key management packets and
- decapsulating the data packets encapsulated into the specific packet format.

15. [original] A method according to claim 14, wherein the step of encapsulating data packets that are not key management packets comprises the substeps of

- encapsulating data packets that are not key management packets into a key management packet format specified by the Internet Key Exchange protocol which defines a certain Initiator Cookie field and
- inserting into the Initiator Cookie field of an encapsulated data packet a value indicating that the encapsulated packet is a data packet and not a key management packet.

16. [previously amended] A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network including intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion and where a security protocol exists comprising a key management connection, the method comprising the steps of

- a method for determining what network address translations, if any, occur on

packets transmitted between said first computer device and said second computer device:

establishing a key management connection according to said security protocol between said first computer device and said second computer device;

composing an indicator packet with a header part and a payload part of which both comprise the network addresses of said first computer device and said second computer device as seen by the node composing said packet;

transmitting and receiving said indicator packet within said key management connection; and

comparing in the received indicator packet the addresses contained in said header part and said payload part, and

- using the information concerning the determined occurrences of network address translations for securely communicating packets between ~~the~~ said first computer device and said second computer device.

17. [original] A method according to claim 16, wherein the security protocol determines a standard port number for a key management connection, and the method further comprises the step of comparing in the received indicator packet a source port number against said standard port number for a key management connection.

18. [previously amended] A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network including intermediate computer devices,

where:

at least one of said computer devices performs a network address translation and/or a protocol conversion;

and wherein a security protocol is acknowledged which determines transport-mode processing of packets for transmission and reception;

and wherein a high-level protocol checksum has been determined for checking the integrity of received packets,

the method comprising the steps of:

- at said first computer device, performing transport-mode processing for packets to be transmitted to said second computer device,
- at said second computer device, performing transport-mode processing for packets received from the first computer device, said transport-mode processing comprising the decapsulation of received packets and
- at said second computer device, updating said high-level protocol checksum for decapsulated packets for compensating for changes, if any, caused by network address translations.

19. [previously amended] A method according to claim 18, wherein

- the step of performing transport-mode processing at said first computer device for packets transmitted to said second computer device takes the form of performing transport-mode processing as determined in the IPSEC protocol suite, and
- the step of performing transport-mode processing at said second computer device for packets received from said first computer device takes the form of performing transport-mode processing as determined in the IPSEC protocol suite.

20. [previously amended] A method according to claim 18, additionally comprising the steps of

- at said first computer device, after performing transport-mode processing for a packet to be transmitted to the second computer device, if network address translations and/or protocol conversions will occur on said packet in transmission to said second computer, encapsulating the processed packet into a packet conforming to a certain second protocol, which second protocol is capable of traversing network address translations and/or protocol conversions, and
- at said second computer device, before performing transport-mode processing for a packet received from said first computer device, decapsulating the received packet from the packet conforming to said second protocol and replacing a number of network addresses in the decapsulated packet with a corresponding number of network addresses taken from the received packet before decapsulation.

21. [original] A method according to claim 18, wherein the step of updating the high-level protocol checksum takes the form of recomputing the checksum for the transport-mode-processed packets.

22. [previously amended] A method according to claim 18, wherein the method additionally comprises the step of obtaining information about the network addresses of first and second computer devices before and after network address translations, and the step of updating the high-level protocol checksum takes the form of incrementally updating the checksum based on the obtained information about the network addresses

of the first and second computer devices before and after network address translations.

23. [previously amended] A method for maintaining the unchanged form of address translations performed by network address translation devices on encapsulated actual data packets transmitted with certain address information between a first computer device and a second computer device through a packet-switched data transmission network, the method comprising the step of

- forcing at least one of said first computer device and said second computer device to transmit to the other computer device keepalive packets with address information identical to that of actual data packets at a high enough frequency so that network address translation devices constantly reuse the mappings used for network address translation even when a certain fraction of the packets communicated between said first computer device and said second computer device are lost in the network.

Please add the following new claims:

24. [new] A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said intermediate computer devices may perform a network address translation and/or a protocol conversion resulting in alteration of a packet propagating therethrough, the method comprising the steps of

- determining what network address translations or protocol conversions, if any, occur on packets transmitted in a data path between said first computer device and said second computer device on packets transmitted between said first computer device and said second computer device,

- if it is found that network address translations and/or protocol conversions occur in said data path between said first computer device and said a second computer device, taking packets conforming to a first protocol and using said first computer device to encapsulate them into packets conforming to a second protocol, said second protocol being capable of traversing network address translations and protocol conversions,

- transmitting said packets conforming to said second protocol from said first computer device to said second computer device.

25. [new] The method of claim 24 further comprising the step of determining if said second computer device supports a secure data communication protocol prior to performing said step of determining what, if any, network address translations and/or protocol conversions are occurring in communications between said first computer device and said second computer device.

26. [new] The method of claim 24 wherein the step of determining what, if any, network address translations or protocol conversions are occurring in communications between said first computer device and said second computer device is accomplished by:

sending at least one IKE Phase 2 Quick Mode message packet from said first computer device to said second computer device including in its private payload section IP addresses for an initator and responder as seen by said first computer device, where one of said first and second computer devices is said initiator and the other of said first and second computer devices is said responder; and

receiving at least one IKE Phase 2 Quick Mode message packet from said second computer device which was sent by said first computer device and including in its private payload section IP addresses for said initator and said responder as seen by said second computer device; and

in said first computer device, comparing said IP addresses in said header(s) of said at least one IKE Phase 2 Quick Mode message packet(s) received from said second computer device to said IP addresses in said private payload section, and, if there is a difference, concluding that a network address translation or a protocol conversion or both have occurred on the data path between said first computer device and said second computer device.

27. [new] The process of claim 26 further comprising the step of periodically transmitting keepalive packets from said first computer device to said second computer device if it is determined that NAT or protocol conversions or both are occurring with the interval between said keepalive packets being set to insure that mappings of said NAT or protocol conversions or both stay the same.

28. [new] The method of claim 24 wherein the step of determining what, if any, port translations are occurring in communications between said first computer device and said second computer device is accomplished by comparing the port number in a packet header for a packet of a protocol that can withstand port translations and which encapsulates an IKE protocol packet sent from said second computer device to said first computer device, and if said port number is not a port number associated with the IKE protocol, concluding that one or more port translations is occurring on a data path between said second computer device and said first computer device.

29. [new] A method for receiving data transmitted in tunneled, secure packets sent from a first computer device to a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said intermediate computer devices may perform a network address translation or a protocol conversion resulting in alteration of a packet propagating therethrough, and wherein said tunneled, secure packets comprise packets of a first secure protocol encapsulated in packets of a second protocol which can pass through network address translations or protocol conversions, the method comprising the steps of:

- decapsulating packets received from said first computer device and conforming to said second protocol to recover packets conforming to said first protocol; and

- using said first secure protocol to recover data transmitted in said first secure protocol packets.

30. [new] A method for conditionally setting up a secure communication connection and communicating data between a first computer device and a second computer device through a packet-switched data transmission network including intermediate computer devices, where at least one of said computer devices performs a network address translation or a protocol conversion or both a protocol conversion and a network address translation, the method comprising the steps of:

carrying out a negotiation between said first and second computer devices to determine if said second computer device supports a secure communication protocol which is incompatible with network address translations or protocol conversions or both;

as a response to a finding indicating that the second computer device supports said secure communication protocol, setting up a secure communication connection between said first computer device and said second computer device in which communication connection said secure communication protocol is employed;

as a response to a finding indicating that said second computer device does not support said secure communication protocol, disabling use of said secure communication protocol between said first and said second computer devices;

if it is found that said second computer device supports said secure communication protocol, determining what network address translations or protocol conversions or both, if any, occur on packets transmitted between said first computer device and said second computer device;

if it is found that network address translations or protocol conversions occur on packets transmitted between said first computer device and said second computer device, taking packets that conform to said secure communication protocol and encapsulating them into packets that conform to a second protocol, which second protocol is capable of traversing network address translations or protocol conversions, or both without violating said second protocol;

if it is found that network address translations or protocol conversions occur on packets transmitted between said first computer device and said second computer device, periodically transmitting keepalive packets from said first computer device to said second computer device with the interval between said keepalive packets being set to insure that mappings of said NAT or protocol conversions or both stay the same;

transmitting said packets conforming to said second protocol from said first computer device to said second computer device.

31. [new] The method of claim 30 wherein said secure communication protocol is the IPsec protocol, and said second protocol is either the TCP or UDP protocol.

32. [new] The method of claim 30 wherein said step of determining if said second computer device supports a secure communication protocol includes the step of finding out whether said second computer supports the IPsec protocol, and wherein said step of determining what network address translations or protocol conversions or both, if any, occur on packets transmitted between said first computer device and said second computer device comprises the steps:

sending at least one IKE Phase 2 Quick Mode message packet from said first computer device to said second computer device including in its private payload section IP addresses for an initator and responder as seen by said first computer device, where one of said first and second computer devices is said initiator and the other of said first and second computer devices is said responder; and

receiving at least one IKE Phase 2 Quick Mode message packet from said second computer device which was sent by said first computer device and including in its private payload section IP addresses for said initator and said responder as seen by said second computer device; and

in said first computer device, comparing said IP addresses in said header(s) of said at least one IKE Phase 2 Quick Mode message packet(s) received from said second computer device to said IP addresses in said private payload section, and, if there is a difference, concluding that a network address translation or a protocol conversion or both have occurred on the data path